DPDP-Readiness Checklist — an operational aid for Indian digital businesses

> **What this is / is not.** This is general, illustrative and **non-exhaustive** information on the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Rules made under it. It is **not legal advice**, **not a compliance certification or determination**, and does **not** create an advocate–client relationship. Not every item below applies to every business, and some obligations are still being phased in by notification. It is a readiness *prompt* for a qualified team — a real assessment needs the facts of your own processing. **Confirm commencement, exemptions, designation notifications and sector rules for your own entity before acting.** Current as at 1 August 2026.
>
> *Prepared by Rushikesh Mahajan, Advocate.*

Start here — know your data (before any checklist)

- [ ] **Data map / RoPA** — list your systems, the personal data in each, the purpose(s), who it comes from, who you share it with (and their role), where it's stored, and the deletion trigger. Every item below assumes you've done this first.
- [ ] **Classify each recipient** — for every party you share data with, decide: is it a **Processor** (acts on your behalf) or an **independent Data Fiduciary** (decides its own purposes)? The obligations differ, and getting this wrong is the most common early error.

Core checklist — applies to most Data Fiduciaries

- [ ] **Lawful basis** (s.4(1)) — every *purpose* runs on either consent (s.6) **or** a listed legitimate use (s.7). Map each distinct purpose to one documented basis; split mixed-purpose flows. ("Lawful purpose" = any not expressly forbidden by law, s.4(2).)
- [ ] **Notice** (s.5(1)) — accompanies/precedes a consent request; states (i) the personal data + purpose, (ii) how to withdraw (s.6(4)) and raise a grievance (s.13), (iii) how to complain to the Data Protection Board. Offer the notice in English + any Eighth-Schedule language the principal chooses (s.5(3)).
- [ ] **Consent** (s.6(1)) — free, specific, informed, unconditional, unambiguous, clear affirmative action; limited to the data necessary; as easy to withdraw (s.6(4)) as to give; no bundling; no dark patterns. On withdrawal you **and your processors** cease within a reasonable time (s.6(6)).
- [ ] **Consent record / burden of proof** (s.6(10)) — the burden is on **you** to prove notice was given and consent obtained. Log timestamp, notice-version, purpose, and data items per consent event.
- [ ] **Purpose limitation** — use data only for the notified purpose. For a **new** purpose, reassess the lawful basis, update the notice where needed, and obtain fresh consent *where consent is the basis relied on*.
- [ ] **Data-principal rights** (ss.11–14) — working intake for access (s.11), correction/completion/erasure (s.12), grievance (s.13), nomination (s.14): request channel, identity check, response content, an owner, an evidence log, and an escalation route.

- [ ] **Published contact** (s.8(9)) — publish the business contact of a Data Protection Officer (**if you are a Significant Data Fiduciary**) **or** of a person able to answer principals' questions. *(A non-SDF publishes a contact person — that is not a statutory "DPO".)*
- [ ] **Grievance mechanism** (s.8(10)) — an effective, responsive redress mechanism (confirm the current Rules' timeline for your entity).
- [ ] **Accuracy** (s.8(3)) — where data is used to make a decision affecting the principal, or disclosed to another Data Fiduciary, keep it complete, accurate and consistent.
- [ ] **Security safeguards** (s.8(4)-(5)) — reasonable technical + organisational measures: not only encryption/access-control/logging but also detection, patching, backup-restoration, security testing, and a vendor breach-notification SLA.
- [ ] **Breach response** (s.8(6) + Rule 7, DPDP Rules 2025) — two clocks: **initial intimation to the Board without delay**, then a **detailed report to the Board within 72 hours** of becoming aware; **and** notify **each affected principal** of the breach. Have templates and role-owners ready.
- [ ] **Retention & erasure** (s.8(7)) — erase when the purpose is served or consent is withdrawn (and cause your processor to erase) **unless** a law requires you to keep it. Keep a **record-category retention schedule** (purpose-expiry vs statutory/legal holds — e.g. tax, KYC/AML, claims, litigation) so erasure and mandatory retention don't collide.
- [ ] **Processor contracts** (s.8(2)) — engage a processor only under a **valid contract** (the Act's requirement; best practice = written and auditable). Under s.8(1) you remain accountable to the Board for processing done on your behalf, irrespective of contract terms.
- [ ] **Children & guardianship** (s.9) — for users under 18 **or** persons with a lawful guardian: verifiable parental/guardian consent (s.9(1)); nothing likely to harm a child's well-being (s.9(2)); no tracking, behavioural monitoring or targeted ads to children (s.9(3)).
- [ ] **Cross-border** (s.16) — negative-list model: transfer allowed unless the Central Government restricts the destination; sectoral localisation (RBI/IRDAI) overrides (s.16(2)).
- [ ] **SDF watch** (s.10) — high volume/sensitivity may attract Significant-Data-Fiduciary **designation** (by government notification — not a fixed public threshold): then DPIA, periodic independent audit, and a **DPO based in India, responsible to the Board** (s.10(2)).
- [ ] **Consent Manager — future-readiness** (s.6(7)-(9)) — being phased in; design so a Board-registered Consent Manager can later interoperate. Monitor the notifications rather than build to a fixed spec today.

> *Sector notes below are overlays on the Core checklist — not standalone. "Where relying on consent," a purpose-by-purpose basis assessment (including emergency, employment and legally-mandated processing) still governs. "Also check" flags the adjacent regime a business in that sector most often misses.*

1. Healthtech / digital health

Priority focus: health/wellness data at scale — high harm if breached; a realistic SDF-designation candidate.

- [ ] Consent (s.6) + notice (s.5) per care journey (diagnostics, records, tele-consult).

- [ ] Classify each actor (lab, clinic, doctor, cloud/AI vendor) as fiduciary or processor — don't assume "processor"; contract accordingly (s.8(2)).
- [ ] Verifiable parental/guardian consent (s.9(1)) for any under-18 patient data.
- [ ] Reconcile s.8(7) erasure with clinical-record retention (the "law requires retention" carve-out).
- [ ] Breach playbook (s.8(6)/Rule 7) + tight record access-control (s.8(5)); SDF prep (DPIA + audit + India DPO, s.10) at scale.
- [ ] **Also check:** ABDM/ABHA participation terms + telemedicine/EHR and clinical-record-retention rules.

2. Fintech (lending / payments / wealth)

Priority focus: financial data across bureaus, co-lenders, account aggregators, collection partners.

- [ ] **Classify each party first** — bureaus, co-lenders and account aggregators are often **independent Data Fiduciaries, not your processors**. Use processor terms (s.8(2)) only where a party acts on your behalf; for fiduciary-to-fiduciary sharing, document the basis, notice and responsibility separately.
- [ ] Consent (s.6), *where relied on*, specifically for bureau pulls / co-lending shares — no bundling.
- [ ] Accuracy duty (s.8(3)) bites hard — credit/underwriting decisions "affect the principal".
- [ ] No cross-sell reuse of borrower data without a fresh basis (s.4 / s.6).
- [ ] RBI overlay (payment-data localisation, AA consent, digital-lending, outsourcing) preserved over s.16 by s.16(2).
- [ ] Retention schedule honouring KYC/AML/PMLA statutory holds vs purpose-expiry; SDF watch (s.10).
- [ ] **Also check:** SEBI obligations for the wealth/advisory product + CIC (credit-information) correction duties.

3. Insurtech

Priority focus: financial + health data via POSPs/agents, shared with insurers.

- [ ] Consent + notice (ss.5–6) at the point of sale, not post-issuance.
- [ ] Role allocation: insurer vs intermediary vs TPA — contract each on its actual role (s.8(2)).
- [ ] Retention mapped to quotation / underwriting / servicing / **claims + fraud + legal-hold** — not just "policy lifecycle".
- [ ] Data-principal rights (ss.11–14) across the distribution chain (who answers an access request?).
- [ ] **Also check:** IRDAI record-localisation, cyber-security and outsourcing requirements (s.16(2)).

4. HR-tech (recruitment / workforce / background verification)

Priority focus: candidate + employee PII at scale; background verification is among the most sensitive processing.

- [ ] Don't over-read the s.7(i) employment legitimate-use: it covers safeguarding the *employer* (loss/liability, espionage, trade-secret/IP/confidentiality, services to an employee) — **not** the platform's own or candidate-stage processing → get candidate **consent** (s.6) there.

- [ ] Assess employer-purpose vs platform-purpose separately; notice for workplace monitoring / biometric attendance / device telemetry.
- [ ] Challenge-and-correction flow before any adverse BGV decision (s.8(3), s.12).
- [ ] Retention split for rejected candidates vs former employees; s.8(2) contracts with every verification source.
- [ ] **Also check:** cross-border (s.16) if clients/data sit abroad.

5. Adtech / Martech / customer-data platforms

Priority focus: behavioural + identity data and profiling.

- [ ] Consent (s.6) for tracking/profiling that is genuinely free and unambiguous — **no dark patterns**.
- [ ] Per client, fix who is Fiduciary vs Processor and paper it (s.8(2)); map the end-to-end signal + recipient chain.
- [ ] Propagate withdrawal/deletion downstream; maintain suppression lists; rights (ss.11–14) reach the underlying individuals.
- [ ] No behavioural monitoring or targeted ads to children (s.9(3)).
- [ ] **Also check:** cookie/device-ID consent signals + dark-pattern / commercial-communication (consumer-protection) rules.

6. Edtech

Priority focus: children's data — DPDP's strictest area (s.9).

- [ ] Verifiable parental/guardian consent for under-18 learners (s.9(1)); **age-gating alone ≠ parental verification**.
- [ ] No behavioural tracking/monitoring or targeted ads to children (s.9(3)); nothing detrimental to well-being (s.9(2)).
- [ ] Separate school / parent / learner / vendor roles; specific controls for proctoring (biometrics/video/audio) and classroom recordings.
- [ ] Consent + notice (ss.5–6), purpose limitation, learner-exit deletion; s.8(2) vendor contracts.
- [ ] **Also check:** any notified child-processing exemptions and their conditions (s.9(4)–(5)).

7. Consumer AI apps

Priority focus: large user-data volumes; personalisation and model-training as distinct purposes.

- [ ] State model-training as its **own** purpose; identify the basis for it (consent for optional reuse; distinguish inference *necessary to provide a requested feature*, and genuinely anonymised data). Give a separate opt for optional training.
- [ ] Working access/correction/erasure at scale (ss.11–12); map whether erasure can propagate through logs, retrieval/index stores, training/eval sets and model artefacts.

- [ ] Accuracy review (s.8(3)) for consequential decisions; watch inferred/third-party personal data in prompts/outputs.
- [ ] Children's controls (s.9) if minors can use it; s.8(2) contracts + vendor secondary-use limits; breach playbook (s.8(6)).
- [ ] **Also check:** human-review and vendor secondary-use terms for any third-party model API.

8. Mobility / logistics

Priority focus: location, trip and gig-worker data, shared with fleets/partners.

- [ ] Consent + notice (ss.5–6) for location/trip data; granular background-location controls; purpose limitation on movement data.
- [ ] Separate rider / driver / fleet / safety processing; surveillance-notice for driver telematics/camera/audio.
- [ ] Retention by record class (trip history vs accident/insurance/tax holds) — account closure alone isn't a deletion trigger; log any law-enforcement disclosures.
- [ ] s.8(2) contracts with fleet operators and gig-workforce systems; rights (ss.11–14) for riders/drivers; breach playbook (s.8(6)).
- [ ] **Also check:** emergency and law-enforcement disclosure handling.

> *End. Each sector overlay above must travel **with** the Core checklist + this disclaimer — never as a standalone page. This is a readiness prompt, not a compliance determination.*